**Task 1: Identify the critical elements of a GRC framework that Nerdnest needs to implement**

**1. Key components of a GRC framework Nerdnest should include:**

* **Governance**
  + Define roles and responsibilities for cybersecurity oversight.
  + Establish security policies and procedures.
  + Align cybersecurity goals with business objectives.
* **Risk Management**
  + Implement a structured risk assessment process.
  + Develop a risk register to track identified risks.
  + Prioritise risks based on impact and likelihood.
  + Apply mitigation strategies and controls.
* **Compliance**
  + Monitor relevant laws and industry standards (e.g., SOX, HIPAA, CCPA).
  + Create standard operating procedures to meet compliance obligations.
  + Conduct regular audits and maintain evidence of compliance.

**2. How risk assessment helps Nerdnest:**

Conducting a comprehensive risk assessment allows Nerdnest to:

* Identify internal and external threats (e.g., phishing, data breaches).
* Discover vulnerabilities in its infrastructure, policies, and procedures.
* Evaluate potential impact and likelihood of threats.
* Prioritise remediation efforts and allocate resources effectively.
* Align its risk management strategy with industry best practices such as NIST RMF or ISO 27005.

**3. Importance of continuous monitoring:**

* Ensures real-time visibility into systems and processes.
* Detects policy violations, system anomalies, or indicators of compromise early.
* Supports ongoing compliance with evolving regulations and standards.
* Provides actionable insights for proactive threat mitigation.
* Demonstrates due diligence to regulators and stakeholders.

**Task 2: Identify and apply the ITIL processes to Nerdnest**

**1. Key ITIL processes to include:**

* **Incident Management**
* **Problem Management**
* **Change Management**
* **Service Request Management**
* **Service Level Management**
* **Configuration Management**
* **Release and Deployment Management**
* **Continual Improvement**

**2. How ITIL helps Nerdnest:**

Adopting ITIL enables Nerdnest to:

* Standardise and streamline IT operations.
* Align IT services with business needs and objectives.
* Improve response times and service delivery quality.
* Reduce downtime through proactive incident and problem management.
* Foster a culture of continual improvement and accountability.

**3. Importance of Change Management:**

* Ensures all changes are evaluated for impact and risk before implementation.
* Minimises service disruptions and unplanned outages.
* Provides a formal approval process to maintain control.
* Enhances communication and coordination across teams.

**4. How to incorporate Change Management in ITIL:**

* Define a **Change Advisory Board (CAB)** for change evaluation and approval.
* Use **change request forms** with documented risk analysis.
* Categorise changes (standard, normal, emergency).
* Maintain a **change schedule (Forward Schedule of Change)**.
* Track change outcomes to improve the process over time.

**Task 3: Identify and apply laws related to Nerdnest's operations**

**1. Role of SOX:**

* Enforces accurate and transparent financial reporting.
* Requires internal controls to prevent fraud or misstatements.
* Nerdnest must ensure data integrity and access controls over financial systems.
* Non-compliance can result in fines and loss of investor confidence.

**2. Impact of HIPAA:**

* Applies if Nerdnest handles healthcare data (e.g., through partnerships or services).
* Requires safeguards like encryption, access controls, and audit logs.
* Administrative, physical, and technical safeguards must be in place.
* Regular staff training and risk assessments are also mandatory.

**3. CCPA & CPRA impact:**

* Require transparency about data collection and sharing practices.
* Nerdnest must allow California residents to access, delete, or opt out of data sharing.
* CPRA expands data subject rights and mandates a risk-based approach to privacy.
* Failing to comply can result in significant fines and class-action lawsuits.

**Task 4: Cybersecurity audits**

**1. Benefits of regular cybersecurity audits:**

* Validate the effectiveness of security controls and policies.
* Identify vulnerabilities and misconfigurations early.
* Maintain regulatory compliance (e.g., HIPAA, SOX, CCPA).
* Increase stakeholder confidence in Nerdnest’s cybersecurity posture.
* Drive continual improvement in security and risk management practices.

**2. How Nerdnest can prepare:**

* Define the scope and objectives of the audit.
* Gather and document current security policies, procedures, and controls.
* Ensure access to logs, risk assessments, and compliance evidence.
* Conduct an internal pre-audit or gap analysis.
* Train staff to respond to auditor inquiries confidently and accurately.